

**UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ALABAMA
WESTERN DIVISION**

SHARON STANDIFER,)	
individually and d/b/a)	
SUPERIOR OFFICE SOLUTIONS,)	
)	
Plaintiff,)	7:16-cv-01176-LSC
)	
vs.)	
)	
BEST BUY STORES, L.P.,)	
)	
Defendant.)	

MEMORANDUM OF OPINION

Before the Court is Plaintiff Sharon Standifer's ("Standifer") motion for partial summary judgment (doc. 37) and Defendant Best Buy Stores, L.P.'s ("Best Buy") motion for summary judgment (doc. 39). The motions have been fully briefed and are ripe for review. For the reasons stated below, Standifer's motion for partial summary judgment (doc. 37) is due to be GRANTED in PART and DENIED in PART and Best Buy's motion for summary judgment (doc. 39) is also due to be GRANTED in PART and DENIED in PART.

I. BACKGROUND¹

Standifer is the sole owner and proprietor of Superior Office Solutions (“SOS”), an accounting and business consulting company. To conduct business, Standifer would sometimes use her husband’s computer. On August 14, 2015, Standifer’s husband was using his computer when he opened a file and a blue screen appeared. The next day, Standifer took the computer to a Best Buy location in Tuscaloosa, Alabama to be repaired. Although Standifer had previously purchased accessories, such as cables, videos, and TVs, from Best Buy, she had never before used its Geek Squad’s computer services. Her knowledge of Best Buy’s computer sales and services came exclusively from general advertisements.

While at Best Buy, Standifer decided to replace her husband’s computer with a new Lenovo computer instead of having the original computer repaired. She purchased the computer for \$557.24 and requested that Best Buy transfer all of the data from the original computer to the Lenovo. This data included information about

¹ The facts set out in this Opinion are gleaned from the parties’ submissions of facts claimed to be undisputed, their respective responses to those submissions, and the Court’s own examination of the evidentiary record. These are the “facts” for summary judgment purposes only. They may not be the actual facts. *See Cox v. Adm’r U.S. Steel & Carnegie Pension Fund*, 17 F.3d 1386, 1400 (11th Cir. 1994). The Court is not required to identify unreferenced evidence supporting a party’s position. As such, review is limited to exhibits and specific portions of the exhibits specifically cited by the parties. *See Chavez v. Sec’y, Fla. Dept. of Corr.*, 647 F.3d 1057, 1061 (11th Cir. 2011) (“[D]istrict court judges are not required to ferret out delectable facts buried in a massive record . . .”) (internal quotations omitted).

several of her clients. As part of the transaction, Standifer entered into a Data Services Agreement with Best Buy, which provided that Best Buy would set up Standifer's new computer, install software on the computer, and complete the requested data transfer. The Data Services Agreement included several waivers and disclaimers, which stated that Geek Squad would not be liable for any indirect, incidental, or consequential damages. Best Buy then retained possession of Standifer's original computer from August 15, 2015 to August 24, 2015. At no point did Standifer ask or Best Buy explain how the data from the original computer would be securely transferred to the Lenovo computer.

On August 20, 2015, Best Buy sent Standifer an email stating that her computer had reached the "Ultimate Fix-It Stage" and that a Geek Squad Agent was actively repairing her device. (*See* Doc. 49-4.) After being informed by Best Buy employees that the data transfer between her original computer and the Lenovo had not yet occurred, Standifer cancelled the data transfer, picked up her old computer, and received a full refund. Standifer then purchased a new computer from Tuscom, the business where Standifer had purchased her original computer, and Tuscom transferred the data from the original computer to the new one.

On November 24, 2015, Phil Simpson ("Simpson"), a captain with the Tuscaloosa Police Department, notified Standifer that data stored on her original computer had been found on his father's iMac. Both Simpson and his father had

viewed certain files belonging to Standifer. Simpson's father had purchased the iMac from Best Buy's Tuscaloosa location in October 2015. According to a Forensic Investigation Report, the data from Standifer's computer was copied to the Simpson computer on August 23, 2015, while both computers were in Best Buy's possession. Many of the files were then moved to another folder, labeled "geekSQUAD BACKUP," on October 21, 2015, which is the day that Simpson's father picked up the computer from Best Buy. However, it remains unclear how Standifer's information ended up on the Simpson computer. Although Standifer's expert was able to determine when the data transfer occurred, his report does not include evidence as to who transferred the data. Moreover, Best Buy has no records that Standifer's computer was ever hooked up for data services.²

The data found on the Simpson computer included files containing sensitive information about Standifer and her clients. Among these files were Standifer's personal tax returns, the tax returns of some of her clients, and documents regarding Standifer's sister's medical history. Standifer admits that aside from a log-in password she had not independently password protected most of these documents.

² Best Buy's data transfer services are guided by a Data Services SOP, which explains the process that should be used to transfer data from one computer to another. The Data Services SOP indicates that the preferred method is to use a specifically designed transfer device—dubbed "the Mule"—to serve as an intermediary when transferring data between two devices. (See Doc. 49-2 at 2–3.) The Data Services SOP also includes other instructions, such as what to do when one client receives another client's data due to error.

The day after Simpson contacted Standifer, he went with her to Best Buy to inform the store about Standifer's data appearing on his father's computer. Best Buy responded by creating an Incident Management Report, which discussed the allegedly unauthorized transfer. The Incident Management Report refers to the unauthorized transfer as a "data transfer error," and contains a statement from a Best Buy executive that "[i]t would certainly appear we had a hand in this issue." (*See* Doc. 49-5 at BB_33.) On December 3, 2015, Standifer sent a letter to her clients notifying them that their information may have been transferred to the Simpson computer.

The parties largely dispute how the data transfer has affected Standifer both professionally and personally. Standifer has not lost clients, received bad reviews, or seen a reduction in her business's revenue due to the data breach. However, Standifer has testified that she has worked many unbilled hours to protect her client's information by setting up new logins and changing passwords. She also claims to have taken on new clients for fear that her old clients would leave her. Standifer's client, Mark English, has expressed concerns that some suspicious activity on his credit report may have been related to the data transfer. Standifer wrote to three different credit agencies on English's behalf. Standifer also testified that due to her tax returns appearing on the Simpson computer she filled out an affidavit with the

IRS and the State of Alabama. Standifer has indicated that this incident has caused her to suffer from anxiety.

II. STANDARD

Summary judgment is appropriate “if the movant shows that there is no genuine dispute as to any material fact³ and the movant is entitled to judgment as a matter of law.” Fed. R. Civ. P. 56(a). A dispute is genuine if “the record taken as a whole could lead a rational trier of fact to find for the nonmoving party.” *Id.* A genuine dispute as to a material fact exists “if the nonmoving party has produced evidence such that a reasonable factfinder could return a verdict in its favor.” *Greenberg v. BellSouth Telecomms., Inc.*, 498 F.3d 1258, 1263 (11th Cir. 2007) (quoting *Waddell v. Valley Forge Dental Assocs.*, 276 F.3d 1275, 1279 (11th Cir. 2001)). The trial judge should not weigh the evidence, but determine whether there are any genuine issues of fact that should be resolved at trial. *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 249 (1986).

In considering a motion for summary judgment, trial courts must give deference to the non-moving party by “view[ing] the materials presented and all factual inferences in the light most favorable to the nonmoving party.” *Animal Legal Def. Fund v. U.S. Dep’t of Agric.*, 789 F.3d 1206, 1213–14 (11th Cir. 2015) (citing

³ A material fact is one that “might affect the outcome of the case.” *Urquilla-Diaz v. Kaplan Univ.*, 780 F.3d 1039, 1049 (11th Cir. 2015).

Adickes v. S.H. Kress & Co., 398 U.S. 144, 157 (1970)). However, “unsubstantiated assertions alone are not enough to withstand a motion for summary judgment.” *Rollins v. TechSouth, Inc.*, 833 F.2d 1525, 1529 (11th Cir. 1987). Conclusory allegations and “mere scintilla of evidence in support of the nonmoving party will not suffice to overcome a motion for summary judgment.” *Melton v. Abston*, 841 F.3d 1207, 1220 (11th Cir. 2016) (per curiam) (quoting *Young v. City of Palm Bay, Fla.*, 358 F.3d 859, 860 (11th Cir. 2004)). In making a motion for summary judgment, “the moving party has the burden of either negating an essential element of the nonmoving party’s case or showing that there is no evidence to prove a fact necessary to the nonmoving party’s case.” *McGee v. Sentinel Offender Servs., LLC*, 719 F.3d 1236, 1242 (11th Cir. 2013). Although the trial courts must use caution when granting motions for summary judgment, “[s]ummary judgment procedure is properly regarded not as a disfavored procedural shortcut, but rather as an integral part of the Federal Rules as a whole.” *Celotex Corp. v. Catrett*, 477 U.S. 317, 327 (1986).

III. DISCUSSION

Standifer brings claims for breach of contract, breach of fiduciary duty, conversion, fraud, fraudulent suppression, wantonness, and negligence against Best Buy. Best Buy asserts that summary judgment is due to be granted on each of Standifer’s claims both for substantive reasons and because Standifer has failed to

prove her damages. Standifer argues that she is entitled to summary judgment on Best Buy's contributory negligence defense. Each of these arguments will be addressed in turn.

A. Breach of Contract

In order to be successful on her breach of contract claim, Standifer must demonstrate (1) a valid contract binding the parties; (2) her own performance under the contract; (3) Best Buy's nonperformance under the contract; and (4) resulting damages. *See Barrett v. Radjabi-Mougadem*, 39 So. 3d 95, 98 (Ala. 2009). A valid contract requires "an offer and an acceptance, consideration, and mutual assent to terms essential to the formation of a contract." *Ex parte Grant*, 711 So. 2d 464, 465 (Ala. 1997) (quoting *Strength v. Ala. Dep't of Fin., Div. of Risk Mgmt.*, 622 So. 2d 1283, 1289 (Ala. 1993)).

Standifer bases her breach of contract claim on the Data Services Agreement she entered into with Best Buy.⁴ Specifically, Standifer points to the agreement's "Work to Be Completed" provision, which provided that Best Buy would transfer the data from her original computer to the Lenovo computer. Standifer argues that Best Buy's duty under the Data Services Agreement was to safely transfer her data

⁴ Standifer appears to have abandoned any claim that Best Buy was bound by an implied contract. (*See* Doc. 48 at 14 ("Standifer's breach of contract claim is based on an express contract, the Data Services Agreement, with Best Buy.").)

from the original computer to the Lenovo computer. She asserts that Best Buy breached this duty by transferring her data to the Simpson computer. The Court agrees with Standifer that an implied term of the Data Services Agreement was that the data transfer from Standifer's old computer to the new computer would be done securely. Without the expectation that Best Buy would safely conduct the data transfer, Standifer likely would have never allowed Best Buy to perform the agreed upon data services.

However, when she signed the Data Services Agreement, Standifer agreed to the damages waivers contained within the agreement. Alabama law recognizes the freedom to contract and upholds "clearly manifested limitations" in a contract, such as those found within the Data Services Agreement. *See Campbell v. S. Roof Deck Applicators, Inc.*, 406 So. 2d 910, 913 (Ala. 1981). Paragraph 9 of the agreement's terms and conditions provided that Standifer agreed to "[w]aive any consequential or incidental damages against Geek Squad as a result of this service." (*See* Doc. 40-2 at 77.) The Data Services Agreement also includes a limitation of liability clause, which provided that "[in] no event will Geek Squad be liable for any indirect damages whatsoever. To the extent permitted by law, the total liability of Geek Squad to Client under this Agreement [sh]all in no event exceed the total sums paid by Client to Geek Squad." (*See id.* at 76.)

Standifer does not dispute that these clauses are enforceable or that “[i]f, in the process of transferring her data to the [Lenovo], Best Buy had lost some or all of [her data]” that she would have waived any damages. (*See* Doc. 48 at 16.) Instead, she argues that because there is no evidence that the unauthorized transfer occurred as a result of the services contemplated in the Data Services Agreement that the consequential and incidental damages waiver does not apply to her claims. While Standifer’s interpretation of the consequential and incidental damages waiver may be correct, this argument ignores the Data Services Agreement’s limitation of liability clause. That clause provides that “the total liability of Geek Squad to client under this Agreement [sh]all in no event exceed the total sums paid by Client to Geek Squad.” (*Id.* at 76.) The Court finds this provision to be unambiguous. *See Nunnelley v. GE Capital Info. Tech. Solutions-North America*, 730 So. 2d 238, 241 (Ala. Civ. App. 1999) (“Whether a contract is ambiguous is a question of law for the trial judge.”). It limits Standifer’s ability to recover damages for breach of the Data Services Agreement to the \$557.24 that she paid for Best Buy’s services. Because Standifer concedes that she received a full refund, she is not entitled to recover any additional damages under the Data Services Agreement. Therefore, Best Buy is entitled to summary judgment on Standifer’s breach of contract claim.⁵

⁵ Because the Court concludes that Standifer has waived these damages, it need not consider Best Buy’s argument that Standifer could not recover mental anguish damages on the breach of

Best Buy argues that the waivers contained within the Data Services Agreement, particularly the limitation of liability clause, bar Standifer from recovering damages on any of her claims. In support of this, it cites to Alabama case law enforcing contractual provisions that limit liability. *See Campbell*, 406 So. 2d at 913 (“Contracting parties have a right to express the limitations under which they will be bound, and such clearly manifested limitations will be recognized by the courts.”); *Stewart v. Bradley*, 15 So. 3d 533, 543 (Ala. Civ. App. 2008) (enforcing warranty that disclaimed home builders liability for negligence, mental anguish, and implied warranties of habitability and workmanship). However, the limitation of liability clause in the Data Services Agreement is not as unambiguous as the clauses at issue in the cases Best Buy cites. The clause states: “[i]n no event will Geek Squad be liable for any indirect damages whatsoever.” (Doc. 40-2 at 76.) It does not state whether the clause applies only to indirect damages arising out of a breach of the provisions of the Data Services Agreement or if it also applies to all aspects of Geek Squad’s relationship with its customers. This ambiguity presents a question of material fact as to whether the clause bars Standifer from recovering any damages for the unauthorized data transfer. *See Whitetail Dev. Corp. v. Nickelson*, 689 So. 2d

contract claim. With limited exceptions, Alabama law generally prohibits plaintiffs from recovering emotional distress damages in breach of contract actions. *See Molina v. Meritt & Furman Ins. Agency, Inc.*, 207 F.3d 1351, 1360 (11th Cir. 2000).

865, 867 (Ala. Civ. App. 1996) (“When the terms of a contract are ambiguous in any way, however, the determination of the true meaning of that contract is a question of fact for the finder of fact.”).

B. Breach of Fiduciary Duty

The elements of a breach of fiduciary duty claim are “the existence of a fiduciary duty, a breach of that duty, and damage suffered as a result of that breach.” *Aliant Bank v. Four Star Invs., Inc.*, 244 So. 3d 896, 907 (Ala. 2017). The Alabama Supreme Court has held that fiduciary relationships are “not restricted to such confined relations as trustee and beneficiary, partners, principal and agent, guardian and ward, managing directors and corporation, etc.” *Line v. Ventura*, 38 So. 3d 1, 12 (Ala. 2009) (internal citations omitted). Rather, the responsibilities of a fiduciary flow to “all persons who occupy a position out of which the duty of good faith ought in equity and good conscience to arise. It is the nature of the relation which is to be regarded, and not the designation of the one filling the relation.” *Id.* at 12–13. Fiduciary relationships typically arise in one of four scenarios:

(1) when one person places trust in the faithful integrity of another, who as a result gains superiority or influence over the first, (2) when one person assumes control and responsibility over another, (3) when one person has a duty to act for or give advice to another on matters falling within the scope of the relationship, or (4) when there is a specific relationship that has traditionally been recognized as involving fiduciary duties, as with a lawyer and a client or a stockbroker and a customer.

Aliant Bank, 244 So. 3d at 916 (quoting *Swann v. Regions Bank*, 17 So. 3d 1180, 1193 (Ala. Civ. App. 2008)).

Standifer argues that her relationship with Best Buy falls within the first of these four scenarios. As evidence of this relationship, she points to her deposition testimony that she left her computer with Best Buy “in good faith that it was going to be fixed.” (*See* Doc. 38-1 at 45.) She also points out that it is undisputed that she had no knowledge regarding how Best Buy secures and transfers data from one computer to another. According to Standifer, these facts demonstrate that Best Buy had such superior knowledge and influence over her that a fiduciary relationship existed.

Here, it was reasonable for Standifer to trust Best Buy to act as her fiduciary. Although she had limited prior interactions with Best Buy, Standifer had left her computer containing private information with it. While Standifer had not informed Best Buy of exactly what was on her computer, she could reasonably expect Best Buy to use care to prevent her data from being exposed to an unauthorized third party. Contrary to Best Buy’s assertion, its relationship with Standifer was not merely that of a salesperson and customer. Instead, it retained control over Standifer’s information while she waited for the agreed upon data transfer to take place. By doing so, Best Buy assumed responsibility for the data on Standifer’s computer. Standifer had no reason to believe that the level of trust she placed in Best

Buy was misplaced and justifiably relied on Best Buy to protect her information from being exposed. Moreover, Standifer has produced evidence that Best Buy breached this duty when her files were transferred to the Simpson computer. Therefore, summary judgment on the breach of fiduciary duty claims is due to be denied.

C. Conversion

“To sustain a claim of conversion, there must be (1) a wrongful taking; (2) an illegal assertion of ownership; (3) an illegal use or misuse of another’s property; or (4) a wrongful detention or interference with another’s property.” *Drennen Land & Timber Co. v. Privett*, 643 So. 2d 1347, 1349 (Ala. 1994). Conversion can be established by one of two ways. First, a plaintiff could show “that the defendant converted specific personal property to the defendant’s own use and beneficial enjoyment.” *Huntsville v. Golf Dev., Inc. v. Ratcliff, Inc.*, 646 So. 2d 1334, 1336 (Ala. 1994). A plaintiff “could also show that the defendant destroyed or exercised dominion over property to which, at the time of the destruction or exercise of dominion, the plaintiff had a general or specific title and of which the plaintiff was in actual possession or to which the plaintiff was entitled to immediate possession.” *Id.* Although conversion is an intentional tort, “[t]he intent required is not necessarily a matter of conscious wrongdoing. It is rather an intent to exercise a dominion or control over the goods which is in fact inconsistent with the plaintiff’s rights.”

Johnson v. Northpointe Apartments, 744 So. 2d 899, 904 (Ala. 1999) (internal citations and quotations omitted). Thus, “[t]he bare possession of property without some wrongful act in the acquisition of possession, or its detention, and without illegal assumption of ownership or illegal user or misuser, is not conversion.” *Clardy v. Capital City Asphalt Co.*, 477 So. 2d 350, 352 (Ala. 1985).

Here, Standifer asserts that Best Buy wrongfully converted the private information and computer files stored on her computer. Best Buy does not dispute that Standifer’s private information and computer files are personal property that can be subject to a conversion claim. However, there is no evidence that Best Buy converted Standifer’s private information for its own benefit or destroyed Standifer’s computer files and data. Thus, Standifer can only succeed on her conversion claim if Best Buy improperly exercised dominion over Standifer’s private information or computer files to the exclusion of her rights.

Viewing the evidence in the light most favorable to Standifer, the Court cannot say, as a matter of law, that Standifer has failed to show that someone at Best Buy misused her data. The undisputed evidence is that someone transferred Standifer’s computer files to the Simpson computer while Best Buy had possession of both computers. Although Standifer has presented no direct evidence that this was done at the direction of Best Buy, a reasonable jury could infer that it was. Best Buy has presented no evidence that anyone other than it or its employees had access to

these computers at the time of the data transfer. Additionally, the Forensic Investigation Report reveals that on October 21, 2015 Standifer's data was copied from one folder on the Simpson computer to another folder labeled "geekSQUAD BACKUP." (*See* Doc. 49-1.) This may suggest that at some point a Best Buy employee exercised control over the data in a manner that was inconsistent with Standifer's rights.

Moreover, a reasonable jury could find that the unauthorized data transfer seriously interfered with Standifer's possessory interest in the computer files. Although there is no evidence that the unauthorized transfer prevented Standifer from accessing her computer files once the computer was returned, it did prevent Standifer from being able to control who else could access her information. Prior to the unauthorized data transfer, Standifer's possessory interest in her computer files was exclusive in nature. It is at least arguable that Standifer's ability to exclude others from viewing her data is part of what makes the data valuable to her. Without the exclusive right to possess this data, especially the data containing confidential information about her clients, Standifer was likely deprived of her full ownership interest in the transferred data. A rational jury could find that this deprivation was substantial and to the exclusion of Standifer's property rights. Accordingly, Best Buy's motion for summary judgment on Standifer's conversion claims is due to be denied.

D. Fraud

In support of her fraud claim, Standifer asserts that on several occasions between August 21, 2015 and August 24, 2015 Best Buy told her that nothing had been done to her computer and that no data transfer had been performed. She argues that these representations were fraudulent because the evidence demonstrates that her data was transferred to the Simpson computer on August 23, 2015.

The elements of fraud are: “(1) there must be a false representation; (2) the false representation must concern a material existing fact; (3) the plaintiff must rely upon the false representation; and (4) the plaintiff must be damaged as a proximate result.” *Jarrard v. Nationwide Mut. Ins. Co.*, 495 So. 2d 584, 586 (Ala. 1986). “A false representation even if made innocently or by mistake, operates as a legal fraud if it is a material fact that is acted upon with belief in its truth.” *Davis v. Sterne, Agee & Leach, Inc.*, 965 So. 2d 1076, 1091 (Ala. 2007). However, it is not enough for there to be a misrepresentation. In order to recover on a fraud claim, a plaintiff must prove that she acted on the other party’s false representations. *See Hunt Petroleum Corp. v. State*, 901 So. 2d 1, 5 (Ala. 2004). The test for determining whether a plaintiff has relied on a misrepresentation is generally if she would have acted differently in the absence of the representation. *See id.*

Because intent is not a required element of a fraudulent misrepresentation claim, even though Standifer only asserts that Best Buy recklessly made false

statements, she can still succeed on her fraud claim if the other elements for fraudulent misrepresentation have been met. In its reply brief, Best Buy argues that Standifer cannot sustain her fraudulent misrepresentation claim based on the statement that no data transfer had been performed because she only supports this assertion with citations to the allegations in her amended complaint. However, Best Buy admitted in its Answer that its employees made these statements. (*See* Ans. to Am. Compl. ¶¶ 9, 12, 34.) It also admitted these statements in response to Standifer’s “Additional Undisputed Material Facts.” (*See* Doc. 56 at 1 ¶ 5.)⁶ Moreover, it is undisputed that the Incident Management Report documented that on August 24, 2015 Standifer had been informed “that the transfer was still not completed.” (*See* Doc. 49-5 at BB_23.) Thus, the Court will assume that Best Buy employees made these statements.⁷

⁶ The “Additional Undisputed Material Facts” asserted that:

Best Buy’s “employees informed Plaintiff that no data transfer had been performed” over the nine-day period from August 15-24, 2015. (Ans. to Am. Comp. ¶ 9, doc. 19). “[O]n or about August 24, 2015, Plaintiff Standifer was informed that the data transfer between the old computer and the Lenovo computer had not occurred.” (Id. ¶ 12).

(*See* Doc. 48 at 6 ¶ 5.) In its reply brief, Best Buy did clarify that its statement that “no data transfer had been performed” was in response to Standifer’s allegation that “[o]ver the next nine days, Defendant represented to Plaintiffs that the transfer had not been done, but would be done soon.” (*See* Doc. 56 at 1 ¶ 5.)

⁷ Standifer’s Amended Complaint alleges that Best Buy employees made two other fraudulent statements: (1) that Best Buy “could and would” safely transfer the information from her original computer to the Lenovo computer and (2) that the Lenovo computer was being run through virus testing to make sure that its data had not been compromised. (*See* Am. Compl. ¶¶ 33, 35.) Best Buy has not admitted and Standifer has not presented evidence that these statements were ever

Best Buy also argues that these alleged statements were not fraudulent because the evidence indicates that Best Buy never transferred Standifer's data from her original computer to the Lenovo computer. Although it appeared to a Best Buy employee that Standifer's computer had not been touched and there is no record of her computer being hooked up for data services, this does not necessarily mean that there was no data transfer. Other evidence indicates that a data transfer had been attempted. For example, Standifer's expert was able to determine that her data was transferred while in Best Buy's custody. Moreover, Standifer received the "Ultimate Fix-It Stage" email, which stated that a "Geek Squad Agent [was] actively repairing" her old computer. (*See* Doc. 49-4.) This conflicting evidence presents a question of fact as to whether Best Buy had at least begun to perform the contemplated data transfer.

Standifer has also presented evidence that information about what work was being performed on her computer was material to her relationship with Best Buy. Standifer paid Best Buy to transfer data from her computer and information about how that work was progressing was likely central to their relationship. She also testified that she informed Best Buy that it was important to her that the computer

made. Moreover, even if these statements were made, Standifer has presented no evidence that she relied upon them. Therefore, Standifer may not base her fraudulent misrepresentation claims on these purported statements.

files get transferred over to the Lenovo. Further, there remains a question of fact as to whether Standifer reasonably relied on Best Buy's statements. "An essential element of any fraud claim is that the plaintiff must have reasonably relied on the alleged misrepresentation." *Waddell & Reed, Inc. v. United Investors Life Ins. Co.*, 875 So. 2d 1143, 1160 (Ala. 2003). The reliance element of a fraud claim "requires that the misrepresentation actually induced the injured party to *change its course of action*." *Exxon Mobil Corp. v. Ala. Dep't of Conservation & Natural Res.*, 986 So. 2d 1093, 1116 (Ala. 2007) (quoting *Hunt Petroleum*, 901 So. 2d at 4 (Ala. 2004)) (emphasis in original).

After being told that no data transfer had been performed, Standifer picked up her computer from Best Buy and took it to Tuscom. A jury could find that this was a reasonable response to Best Buy's statements that the data transfer had yet to be performed. Moreover, Standifer may have acted differently if Best Buy had not made these statements. As Standifer asserts, if she knew that there had been a data transfer, she could have taken steps to prevent her data from being published to a third party. For example, Standifer might have instructed Best Buy to destroy any data of hers that it had copied while working on her computer. Accordingly, Best Buy's motion for summary judgment on Standifer's fraud claim is due to be denied.

It does not appear to the Court that Standifer is basing her fraudulent misrepresentation claim on any other statement made by Best Buy. To the extent

that Standifer bases her fraud claim on statements contained within the “Ultimate Fix-It Stage” email, these statements are insufficient. The “Ultimate Fix-It Stage” email informed Standifer that her device was being repaired and that she would be kept posted throughout the process. (*See* Doc. 49-4.) Thus, the information contained within the “Ultimate Fix-It Stage” email indicated that a data transfer was being performed. As a matter of law, it would have been unreasonable for Standifer to rely on this email to conclude that Best Buy had not begun work on her computer. Therefore, while Standifer may use the email as evidence that Best Buy’s other statements were false, the email itself cannot serve as a basis for her fraudulent misrepresentation claim.

E. Fraudulent Suppression

Best Buy also moves for summary judgment on Standifer’s fraudulent suppression claim. Standifer alleges that Best Buy suppressed three material facts: (1) that it had worked on her computer and transferred its data to the Simpson computer; (2) that it failed to or was unable to adequately control and protect her confidential computer files; and (3) that her computer files and private information had in fact been transferred to at least one other computer. She asserts that in reliance on the suppression of this information she did not cancel her transaction with Best Buy until August 24, 2015, and as a result of the unauthorized transfer and unreasonable delay, her personal information was disseminated without her consent.

To succeed on a fraudulent suppression claim, a plaintiff must demonstrate: “(1) a duty on the part of the defendant to disclose facts; (2) concealment or nondisclosure of material facts by the defendant; (3) inducement of the plaintiff to act; (4) action by the plaintiff to his or her injury.” *Freightliner, L.L.C. v. Whatley Contract Carriers, L.L.C.*, 932 So. 2d 883, 891 (Ala. 2005) (quoting *Lambert v. Mail Handlers Benefit Plan*, 682 So. 2d 61, 63 (Ala. 1996)). Mere silence is not fraud unless there is some duty to communicate. *See Berkel & Co. Contractors, Inc. v. Providence Hosp.*, 454 So. 2d 496, 505 (Ala. 1984). “The obligation to communicate may arise from the confidential relations of the parties or from the particular circumstances of the case.” Ala. Code § 6-5-102. When looking to the “circumstances of the case” to determine whether there is a duty, courts should look to “(1) the relationship of the parties; (2) the relative knowledge of the parties; (3) the value of the particular fact; (4) the plaintiff’s opportunity to ascertain that fact; (5) the customs of the trade; and (6) other relevant circumstances.” *State Farm Fire & Cas. Co. v. Owen*, 729 So. 2d 834, 842–43 (Ala. 1998).

The Court has already found that Standifer and Best Buy arguably enjoyed a confidential relationship. If so, Best Buy had a duty to disclose material facts regarding the services it was performing on Standifer’s computer. Moreover, even if they were not in a confidential relationship, the “circumstances of the case” supports a finding that Best Buy had a duty to disclose. Best Buy voluntarily entered

into a contract with Standifer to perform the requested data transfer services. Standifer agreed to allow Best Buy to have access to her confidential computer files so that this transfer could be performed. This evidence indicates that their relationship was more consequential than the typical buyer-seller relationship. Additionally, Best Buy would necessarily have more knowledge than Standifer regarding what it had done to her computer and its ability to protect her data during the transfer process. It is undisputed that Standifer was never informed how Best Buy would securely transfer her data. Thus, while Best Buy had protocols for how to transfer client data, she had no knowledge of how the data transfer process worked.

Turning to the remaining relevant factors, these too weigh in Standifer's favor. There can be no dispute that Standifer's private information and customer's data are valuable to her. Thus, if, as Standifer contends, Best Buy knew that it could not adequately protect her information or that it had transferred the information to someone else's computer, this would be valuable information. If Standifer had known about the alleged data transfer, she likely could have taken steps to prevent her information from being disseminated to a third party. Finally, Standifer likely would not have been able to determine that her computer files had been transferred to the Simpson computer or that Best Buy could not adequately protect her private data. The evidence indicates that the only way Standifer could learn that her

computer had been worked on was to ask Best Buy. When Standifer inquired about the status of her computer, she was told that no data transfer had been performed. After evaluating these factors, the Court concludes that there is sufficient evidence to find that Best Buy owed Standifer a duty to disclose the facts that she asserts were suppressed.

Additionally, “[e]ven though one is under no obligation to speak as to a matter, if he undertakes to do so, either voluntarily or in response to inquiries, he is bound not only to [tell the truth], but also not to suppress or conceal any facts within his knowledge which will materially qualify those stated.” *See Jackson Co. v. Faulkner*, 315 So. 2d 591, 600 (Ala. Civ. App. 1975) (internal citations and quotations omitted). Because there is evidence that Best Buy told Standifer that no data transfer had been performed, it had an independent duty to qualify that statement with any other information it had about the work being performed on Standifer’s computer.

Nonetheless, Standifer’s fraudulent suppression claim can only succeed if Best Buy had actual knowledge about the allegedly concealed information. A defendant cannot be liable for fraudulent suppression if it is unaware of the facts that were allegedly suppressed. *See McGarry v. Flourney*, 624 So. 2d 1359, 1360 (Ala. 1993); *see also Harrell v. Dodson*, 398 So. 2d 272, 276 (Ala. 1981) (“As a matter of law, one can only be liable for concealing facts of which one has knowledge.”). Here,

Standifer asserts that the representations within the “Ultimate Fix-it Stage” email combined with the detailed instructions for data transfers contained within the Data Services SOP provides evidence that Best Buy had knowledge of the facts that she alleges were suppressed. However, this evidence does not go toward whether Best Buy *knew* of two of the facts allegedly suppressed: (1) that it had failed to protect her confidential computer files and (2) that her computer files had in fact been transferred to the Simpson computer.

Regardless of whether some action by a Best Buy employee working on Standifer’s computer caused the unauthorized data transfer, there is no evidence before this Court that Best Buy was aware that it had failed to or was unable to adequately protect Standifer’s computer files. Additionally, there is no evidence that Best Buy had knowledge that Standifer’s data had in fact been transferred to another computer. Indeed, all of the evidence points to Best Buy first learning of the improper transfer from Standifer in November 2015. (*See* Doc. 49-5 at BB_23, 29.)

This evidence does, however, indicate that Best Buy may have known that Standifer’s data had been worked on. But Standifer cannot use this evidence to support her suppression claim, which would require Best Buy’s silence on or concealment of material facts. Here, Best Buy was not silent about whether or not a data transfer had occurred. First, Best Buy sent Standifer the “Ultimate Fix-It Stage” email telling her that Best Buy employees were “actively repairing [her] device.”

(*See* Doc. 49-4.) Then, in response to inquiries by Standifer, Best Buy told her that the data had yet to be transferred. While these statements may support Standifer's fraudulent misrepresentation claim, they cannot support her claim that Best Buy suppressed facts material to their transaction. Therefore, Best Buy is entitled to summary judgment on Standifer's fraudulent suppression claim.

F. Negligence and Wantonness⁸

In Count VI of her Amended Complaint, Standifer asserts claims against Best Buy for negligence and wantonness. Best Buy has moved for summary judgment on both of these claims. Standifer has also filed a motion for partial summary judgment on Best Buy's affirmative defense of contributory negligence.⁹ The Court will address each argument in turn.

1. Wantonness

⁸ In her Amended Complaint, Standifer alleged that in the alternative to Best Buy or one of its employees transferring her data to the Simpson computer, Best Buy negligently and/or wantonly allowed a third-party to breach into its internet security system and publish her computer files. (*See* Doc. 18 at ¶ 59.) Standifer does not make this argument in response to Best Buy's motion for summary judgment and has presented no evidence that this occurred. Therefore, Standifer cannot base her negligence and wantonness claims on this allegation.

⁹ Standifer initially also moved for summary judgment on Best Buy's assumption of the risk defense. (*See* Doc. 37 at 7.) In its Response in Opposition, Best Buy agreed to voluntarily withdraw the affirmative defense of assumption of the risk. (*See* Doc. 43 at 2 n.1.) Accordingly, Standifer's motion for summary judgment on Best Buy's affirmative defense of assumption of the risk is due to be granted.

Wantonness is “the conscious doing of some act or the omission of some duty while knowing of the existing conditions *and* being conscious that, from doing or omitting to do an act, injury will likely or probably result.” *Ex parte Essary*, 992 So. 2d 5, 9 (Ala. 2007) (citing *Bozeman v. Cent. Bank of the South*, 646 So. 2d 601 (Ala. 1994)) (emphasis in original). While negligence is characterized as “the inadvertent omission of duty,” wanton misconduct is characterized by the state of mind of consciously taking an action with knowledge that “the doing or not doing of [the act] will likely result in injury” *Id.* (quoting *Tolbert v. Tolbert*, 903 So. 2d 103, 114–15 (Ala. 2004)). “Wantonness is a question of fact for the jury, unless there is a total lack of evidence from which the jury could reasonably infer wantonness.” *Cash v. Caldwell*, 603 So. 2d 1001, 1003 (Ala. 1992).

In support of her wantonness claim, Standifer argues that Best Buy has protocols for the transfer of data, and because her data was found on the Simpson computer, it was clear that these protocols were not followed. She further asserts that Best Buy’s employees, who are trained to follow these protocols, must have known that failure to follow these procedures put her data at risk. According to Standifer, if Best Buy’s procedures for transferring data are properly used a wrongful transfer cannot occur. But this evidence is not enough to sustain Standifer’s wantonness claim. Even assuming Best Buy’s protocols are in place to prevent wrongful transfers, Standifer has presented no evidence that a Best Buy employee knew he

was not following protocol when handling Standifer's computer. Thus, Standifer has no evidence of the state of mind of whoever handled her device.

There is also no evidence in the record that Best Buy was ever aware that it was putting Standifer's data at risk. To be sure, the Data Services SOP includes information about what to do if one client receives data from another client's device. (*See id.* at BB_57.) However, at most, this indicates Best Buy's general awareness that during the data transfer process data from one client's device may inadvertently end up on another client's device. It does not provide evidence that in this instance a Best Buy employee took action that he knew would likely result in Standifer's data being wrongfully transferred. As Standifer has failed to present any evidence that Best Buy or its employees were aware that they were taking action that put her data at risk, her wantonness claim fails as a matter of law. Therefore, Best Buy is entitled to summary judgment on Standifer's wantonness claim.

2. Negligence

Negligence "is the failure to do what a reasonably prudent person would have done under the same or similar circumstances, or the doing of something that a reasonably prudent person would not have done under the same or similar circumstances." *Ford Motor Co. v. Burdeshaw*, 661 So. 2d 236, 238 (Ala. 1995) (citing *Elba Woods Prods., Inc. v. Brackin*, 356 So. 2d 119 (Ala. 1978)). "To establish negligence, [a] plaintiff must prove: (1) a duty to a foreseeable plaintiff;

(2) breach of that duty; (3) proximate causation; and (4) damage or injury.” *Martin v. Arnold*, 643 So. 2d 564, 567 (Ala. 1994) (citing *Albert v. Hsu*, 602 So. 2d 895, 897 (Ala. 1992)).

Best Buy argues that there is no evidence that it had a duty to safeguard the data on Standifer’s computer. In general, “every person owes every other person a duty not to hurt him.” *Smitherman v. McCafferty*, 622 So. 2d 322, 324 (Ala. 1993) (quoting *Southeastern Greyhound Lines v. Callahan*, 13 So. 2d 660, 663 (Ala. 1943)). “In determining whether a duty exists in a given situation . . . courts should consider a number of factors, including public policy, social considerations, and foreseeability. The key factor is whether the injury was foreseeable by the defendant.” *DiBiasi v. Joe Wheeler Elec. Membership Corp.*, 988 So. 2d 454, 461 (Ala. 2008) (quoting *Patrick v. Union State Bank*, 681 So. 2d 1364, 1368 (Ala. 1996)). Furthermore, “the existence of a duty is strictly a legal question.” *Id.* at 460.

There is sufficient evidence to find that Best Buy owed Standifer a duty to exercise ordinary care in handling her data. As Standifer asserts, there is a duty to use due care in the performance of a voluntary undertaking. *See Beasley v. MacDonald Engineering Co.*, 249 So. 844, 846–47 (Ala. 1971). Moreover, the undisputed evidence shows that Best Buy had custody of Standifer’s computer from August 15, 2015 to August 24, 2015. Even though Best Buy may not have known the exact contents of Standifer’s computer files, it was particularly foreseeable that

mishandling the files could cause her injury. It is common for people to include personal information on their computers or to use them to conduct work. This is presumably why Best Buy had procedures for how its employees should handle customer data. Accordingly, Best Buy owed Standifer a duty to exercise reasonable care.

Best Buy also argues that there is no evidence that it breached any duty owed Standifer, or, even if it did, that this conduct caused Standifer's damages. However, Standifer has presented circumstantial evidence from which a reasonable jury could conclude that her data was transferred to the Simpson computer as a result of negligence on the part of Best Buy. The Forensic Investigation Report revealed that Standifer's data was transferred to the Simpson computer on August 23, 2015. Best Buy does not dispute that this transfer occurred while both computers were in its custody. Standifer has also pointed to the Data Services SOP, which provides the protocols and procedures Best Buy employees should use when conducting data transfers. Those procedures indicate that Best Buy employees are supposed to use either the Mule Dock or Flash Drive to perform data transfer services. (*See* Doc. 49-2 at BB_48.) Despite data from Standifer's computer ending up on the Simpson computer, Best Buy has no records of Standifer's computer being hooked up to these devices for data services. A reasonable jury could conclude that Best Buy did not follow its procedures when handling Standifer's data and thus failed to exercise

reasonable care. Moreover, a jury could also find that Best Buy's failure to exercise due care caused the unauthorized data transfer. After learning that data from Standifer's computer had been found on the Simpson computer, a Best Buy executive stated that "[i]t would certainly appear we had a hand in this issue." (*See* Doc. 49-5 at BB_28.) Based on the evidence in the record, a reasonable jury could conclude the same.

Standifer may not, however, recover emotional distress damages on her negligence claim. Under Alabama law, to show entitlement for emotional distress damages in a negligence action, a plaintiff must show that she can satisfy what is known as the zone-of-danger test *City of Mobile v. Taylor*, 938 So. 2d 407, 410 (Ala. Civ. App. 2005) (quoting *Wal-Mart Stores, Inc. v. Bowers*, 752 So. 2d 1201, 1203 (Ala. 1999)). The Alabama Supreme Court recently reaffirmed this principle in *Hamilton v. Scott* where it stated that Alabama "has not recognized emotional distress as a compensable injury or harm in negligence actions outside the context of emotional distress resulting from actual physical injury, or, in the absence of physical injury, fear for one's own physical injury." 97 So. 3d 728, 736 (Ala. 2012) (quoting *AALAR, Ltd., Inc. v. Francis*, 716 So. 2d 1141, 1148 (Ala. 1998)). Standifer has cited the Court to no authority to the contrary. Instead, the case she cites, *Pittman v. Mast Advert. Pub., Inc.*, 619 So. 2d 1377, 1379 (Ala. 1993), includes no discussion about whether emotional distress damages can be recovered in a negligence action

absent physical injury. As Standifer has not produced any evidence that the unauthorized data transfer placed her in any physical danger, she cannot recover emotional distress damages for her negligence claims.

3. Contributory Negligence¹⁰

Under Alabama law, “a plaintiff cannot recover in a negligence suit where [the] plaintiff’s own negligence is shown to have proximately contributed to his damage, notwithstanding a showing of negligence on the part of the defendant.” *Brown v. Piggly-Wiggly Stores*, 454 So. 2d 1370, 1372 (Ala. 1984) (citing *Ala. Power Co. v. Scholz*, 215 So. 2d 447, 452 (1968)). As with negligence, a plaintiff may be found to be contributorily negligent if she failed to act as a reasonably prudent person would. *See H.R.H. Metals, Inc. v. Miller ex rel. Miller*, 833 So. 2d 18, 27 (Ala. 2002) (citing *Sprouse v. Belcher Oil Co.*, 577 So. 2d 443, 444 (Ala. 1991)).¹¹

¹⁰ Unlike with other portions of this Opinion, when considering Standifer’s motion for summary judgment on Best Buy’s contributory negligence defense, the Court considers the evidence in the light most favorable to Best Buy. *See Mize v. Jefferson City Bd. of Educ.*, 93 F.3d 739, 742 (11th Cir. 1996).

¹¹ In the past, Alabama courts have held “[t]he three essential elements of contributory negligence are knowledge of the condition, appreciation of the danger, and failure to exercise reasonable care with such knowledge and appreciation of the danger.” *See Mitchell v. Torrence Cablevision USA, Inc.*, 806 So. 2d 1254, 1257 (Ala. Civ. App. 2000) (citing *Wallace v. Ala. Power Co.*, 497 So.2d 450, 457 (Ala. 1986)). This would appear to conflate the subjective standard of an assumption of the risk defense with the objective standard traditionally associated with contributory negligence. However, the Alabama Supreme Court has since clarified that this subjective standard should only be applied when considering whether a plaintiff was contributorily negligent as a matter of law. *See Horn v. Fadal Machining Ctrs., LLC*, 972 So. 2d 63, 75 (Ala. 2007) (citing *Hannah v. Gregg*,

Best Buy asserts that several actions taken by Standifer contributed to her information being viewed by the Simpsons. It points to the fact that Standifer's husband was the one who originally downloaded the file that caused Standifer to take the computer to Best Buy and that the Forensic Investigation Report revealed that many of the files belonging to Best Buy's clients were stored in a folder bearing Standifer's husband's name. It also points to the undisputed evidence that Standifer was not the only individual who used this computer. Best Buy also faults Standifer for failing to research which store to take her computer to and for choosing Best Buy merely because it was open on a Saturday. Best Buy notes that Standifer knew nothing about the way it secures and transfers data and argues that Standifer never told it that her computer contained confidential or personal information. Best Buy also contends that the reason Standifer's private information and information of her clients were viewed by unauthorized third-parties was that she failed to password protect these files.

Standifer argues that she is entitled to summary judgment on Best Buy's contributory negligence defense because Best Buy has presented no evidence there was a causal connection between these actions and her alleged injury. She also

Bland & Berry, Inc., 840 So. 2d 839, 860–61 (Ala. 2002)); *see also Bielski v. Alfred Saliba Corp.*, 984 F. Supp. 2d 1170, 1176 (M.D. Ala. 2013). When considering Standifer's motion for summary judgment, the Court will apply an objective standard.

contends that Best Buy has not presented any evidence that would indicate she acted negligently or had any duty to act differently than she did. Standifer's primary contention is that none of her actions led to her computer files being transferred to the Simpson computer.

The Court agrees with Standifer that many of the actions Best Buy points to have no bearing on whether or not she was contributorily negligent. The fact that others within Standifer's household were able to access this computer in no way led to Standifer's files being published to the Simpson computer. There is also no evidence that by placing work files in her husband's folder Standifer made it more likely that her data would appear on the Simpson computer. Moreover, while Standifer's husband may have downloaded a virus that required Standifer to bring her computer to Best Buy, this does not suggest any negligence on the part of Standifer.

Similarly, Standifer's failure to research other stores before taking her computer to Best Buy cannot serve as the basis for a contributory negligence defense. The test is whether a plaintiff's actions "proximately contributed" to her injuries. *See Brown*, 454 So. 2d 1370 (Ala. 1984). It does not require a plaintiff to answer for every action she took that ultimately may have led to her injury. For this same reason, any failure by Standifer to notify Best Buy of the information contained on her computer does not meet the causal connection requirement of contributory

negligence. Best Buy has presented no evidence that if this notification had been made it would have taken some action to prevent Standifer's computer files from being published to the Simpson computer. Moreover, Best Buy has presented no evidence that these actions were in fact negligent.

However, a question of fact exists as to whether Standifer's failure to password protect her documents or implement other security measures constitutes contributory negligence. Although Standifer is correct in stating that there is no evidence that this made the unauthorized data transfer more likely to occur, the injury that Standifer complains of is not just that her files were transferred to the Simpson computer. She also seeks damages because these files were viewed by the Simpsons. Although Standifer has pointed to evidence that someone would have to have her login and password before being able to log onto her computer, a reasonable jury could find that Standifer's failure to password protect the individual, confidential files contributed to the Simpsons viewing those files. A reasonable jury could also find that Standifer's failure to take this additional precaution breached the standard of care. Standifer herself testified that she believes that it is a good business practice to password protect confidential client information. (*See* Doc. 40-2 at 12.)

Standifer also owed a duty to secure confidential information on her computer. Standifer argues that Best Buy has not demonstrated that she had this duty because it has not pointed to facts that would have allowed her to foresee that Best

Buy would commit an unauthorized transfer. While a jury may find that Standifer could not have foreseen the data transfer and thus her failure to include additional security measures was reasonable, this does not go toward the element of duty. The relevant duty under the contributory negligence analysis is the duty of a plaintiff to take reasonable precautions for the safety and protection of her own person and property. *See Thomas v. Earnest*, 72 So. 3d 580, 584–85 (Ala. 2011) (noting that passenger in automobile has a duty to exercise reasonable or ordinary care to avoid injury); *Restatement (Second) of Torts* § 463 (1965) (“Contributory negligence is conduct on the part of the plaintiff which falls below the standard to which [she] should conform for [her] own protection”). It was foreseeable to Standifer that a failure to password protect her documents may lead to unwanted parties viewing them. It is for a jury to decide whether the precautions that Standifer did take were reasonable and whether Standifer’s actions proximately contributed to her computer files being viewed by the Simpsons. Therefore, Standifer’s motion for partial summary judgment on her contributory negligence defense is due to be denied.

In its motion for summary judgment, Best Buy argues that evidence of Standifer’s own negligence entitles it to summary judgment on the negligence claim. However, as discussed above, there is a genuine dispute of material fact as to whether Standifer acted negligently and whether those actions contributed to her alleged injury. Moreover, “[t]o establish contributory negligence as a matter of law,

a defendant seeking summary judgment must show that the plaintiff put himself in danger's way and that the plaintiff had a conscious appreciation of the danger at the moment the incident occurred." *Hannah*, 840 So. 2d at 860 (citing *H.R.H. Metals*, 833 So. 2d 18). This is stricter than the standard given to a jury at trial. *Id.* at 861. There, the jury "must decide only whether the plaintiff failed to exercise reasonable care." *Id.*

Here, Best Buy has presented no evidence that Standifer had a conscious appreciation that her actions may have put her data and the data of her clients at risk. Although it is undisputed that Standifer did not password protect all of her files, there is nothing to suggest that Standifer subjectively thought that this could lead to the data being put at risk. Additionally, evidence that Standifer has since updated her business practices does not go toward whether she knew that her business practices at the time the data was transferred to the Simpson computer were inadequate. It is also wholly irrelevant to Best Buy's contention that Standifer was contributorily negligent as a matter of law that in May 2018 Alabama enacted a statute that businesses like Standifer's must "maintain reasonable security measures to protect sensitive personally identifying information against a breach of security." *See* Ala. § 8-38-3. Not only was this statute enacted well after Standifer's data was found on Simpson's computer, but it also does not establish that Standifer appreciated the risks of failing to have adequate security measures. Therefore, the Court does not

find Standifer contributorily negligent as a matter of law, and Best Buy is not entitled to summary judgment on Standifer's negligence claim.

G. Damages

Standifer claims as damages: the actions she undertook to prevent her personal information from being disseminated, the extra work she has put into her business, reputational harm, and mental anguish and emotional distress. (*See* Doc. 48 at 29–31.) Best Buy contends that Standifer cannot recover damages for any of her alleged injuries because they are “solely the result of a perceived and speculative risk of future harm.” (*See* Doc. 40 at 16 (quoting *Shafran v. Harley-Davidson, Inc.*, 07 Civ. 01365(GBD), 2008 WL 763177, at *3 (S.D.N.Y. 2008)).)

It appears that the Alabama state courts have yet to decide the precise issue of what damages consumers may recover when there has been a data breach. However, in various tort cases, the Supreme Court of Alabama has held that “mere fear of a future injury or disease, without more, does not constitute a compensable mental or emotional injury.” *Crutcher v. Williams*, 12 So. 3d 631, 650 (Ala. 2008). Thus, Alabama law does not allow a plaintiff to recover damages if she cannot show that she has suffered actual as opposed to anticipated harm. *See Laurel v. Price*, 154 So. 3d 95, 100 (Ala. 2014). As Best Buy points out, in interpreting their states' adoption of this principle, several other federal district courts have dismissed state-law tort claims where the alleged damages were only based on actions taken due to the fear

of future identity theft. *See, e.g., Muchnik v. Sambodromo, LLC*, Case No. 08-21248-CIV-LENARD/GARBER, 2009 WL 10667067, at *2 (S.D. Fla. May 18, 2009); *Caudle v. Towers, Perrin, Forster & Crosby, Inc.*, 580 F. Supp. 2d 273 (S.D.N.Y. 2008); *Melancon v. La. Office of Student Fin. Assistance*, 567 F. Supp. 2d 873 (E.D. La. 2008).

Ponder v. Pfizer, Inc., 522 F. Supp. 2d 793 (M.D. La. 2007), is illustrative of this line of cases. In *Ponder*, the private data of around 17,000 current and former Pfizer employees were exposed to outsiders in an unauthorized data breach. *See id.* at 794. This data included “the names, social security numbers, and in some instances, addresses and bonus information of Pfizer employees.” *Id.* This information was exposed after an employee installed an unauthorized file-sharing software on his company laptop. *Id.* An investigation conducted by Pfizer revealed that certain files containing employee data had been accessed and copied by an outside third-party. *See id.* A former employee brought a putative class action against Pfizer, alleging that the data breach had caused them damages in the form of “fear and apprehension of fraud, loss of money, and identity theft; the burden and cost of credit monitoring; the burden and cost of closing compromised credit accounts and opening new accounts; the burden of scrutinizing credit card statements and other statements for unauthorized transactions; damage to their credit; loss of privacy and other economic damages.” *Id.* at 795.

The district court dismissed the plaintiff's Louisiana state-law tort claim holding that his complaint failed to allege that he suffered any actual harm from the data breach. *See id.* at 798. The court reasoned that the fear of harm from having information exposed was similar to Louisiana cases where the state courts held that absent "a manifest physical or mental injury or disease" plaintiffs could not recover "for future medical treatment, services, surveillance, or procedures of any kind." *See id.* at 797 (quoting *Bonnette v. Conoco, Inc.*, 837 So. 2d 1219, 1230 n.6 (La. 2003)). The Court further reasoned that although the plaintiff's confidential information had been exposed that he would not suffer any actual damages until the disclosed information had been used to his detriment. *See id.* at 798. Thus, the Court held that the plaintiff could not recover damages for the increased time and effort he had spent monitoring his credit, scrutinizing account statements, and closing and opening accounts because all of these actions were done in the anticipation of future harm. *Id.*

This Court finds the reasoning of the authorities cited by Best Buy to be persuasive and concludes that some of the damages Standifer complains of are unquestionably the result of an anticipated future harm that has never manifested. This includes Standifer taking on new clients and working unbilled hours for fear that her existing clients were going to leave her and updating her business practices to ensure the confidentiality of client information. Standifer has not lost clients,

received bad reviews, or had a loss in revenue as a result of the data transfer. Thus, there is no evidence that Standifer had to undertake the additional hours that she did in order to maintain the level of business that she enjoyed prior to the data transfer.

Standifer argues that her situation is distinguishable from that of the plaintiffs in the cases cited by Best Buy because she has evidence that specific information belonging to her and her clients were exposed to unauthorized third-parties. However, the only known unauthorized parties to view Standifer's data were Simpson, his father, and his sister. There is no evidence that any of these individuals misused or copied any potentially confidential data that they saw. Instead, Simpson was the one who notified Standifer of the data transfer. As the efforts Standifer took to retain client confidence and secure her information were exclusively to prevent an anticipated future harm, she cannot recover damages for these efforts.

The damages Standifer alleges from the work she undertook to inform her clients of the unauthorized data transfer, to notify the State of Alabama and the IRS of a data breach, and to write letters to credit agencies for Mark English present a closer question. A reasonable jury could conclude that those actions were necessary in the wake of the unauthorized data transfer. In his affidavit, English claims that his contact information ended up on several websites and that he attributed this to the Best Buy incident. (*See* Doc. 49-6 at 3.) Although Best Buy correctly notes that there is no evidence that the suspicious activity on English's credit report was caused by

the unauthorized data transfer, English thought that it was related and asked Standifer to write to the credit agencies. Thus, Standifer has presented sufficient evidence that the time and expense of writing those letters was a cognizable damage from the unauthorized data transfer. As Standifer has presented evidence that English “expressed frustration” about the data transfer and had second thoughts about continuing to use her business, she can also seek damages for any of her efforts to retain his particular business.

The same is true for the time and expense Standifer took to write the letter informing her clients about the data transfer. Standifer did not write those letters only in anticipation of future harm, but instead, she also wrote them to inform her clients that the Simpsons had viewed files from her computer. Moreover, as there is evidence that the data breach caused unauthorized third parties to view Standifer’s personal information, it is at least arguable that filling out an affidavit with the IRS and the State of Alabama was necessary. Thus, a jury should decide if Standifer can recover damages for these efforts.

Further, Standifer may recover emotional distress damages unrelated to her fear of potential future harm. Under Alabama law, mental anguish damages are recoverable for both fraud and conversion actions. *See Ford Motor Co. v. Burkett*, 494 So. 2d 416, 418 (Ala. 1986); *Williford v. Emerton*, 935 So. 2d 1150, 1155 (Ala. 2004). Standifer has presented evidence that she was embarrassed because Simpson

was able to access the personal information that she stored on her computer and in fact viewed some of her files. Any embarrassment Standifer suffered due to private information that Simpson actually viewed, could be considered a direct result of the unauthorized data transfer. This is true even though Simpson viewed some of this information while showing Standifer what all was found on his father's computer.

Contrary to Best Buy's assertion, Standifer does not need expert medical testimony to prove these damages. "Under Alabama law, the presence of physical injury or physical symptoms is not a prerequisite for a claim for damages for mental anguish." *Kmart Corp. v. Kyles*, 723 So. 2d 572, 578 (Ala. 1998). "The plaintiff is only required to present some evidence of mental anguish, and once the plaintiff has done so, the question of damages for mental anguish is for the jury." *Id.* (quoting *Ala. Power Co. v. Harmon*, 483 So. 2d 386 (Ala. 1986)). Here, Standifer has testified as to how the data transfer affected her mental state. She has also submitted affidavits from both her sister and friend discussing their observations about the data transfer's effects on Standifer. Thus, although at trial, without expert medical testimony, Standifer may be precluded from presenting evidence that the data transfer caused her to suffer from a particular medical condition, this does not necessarily mean that she is foreclosed from recovering any emotional distress damages.

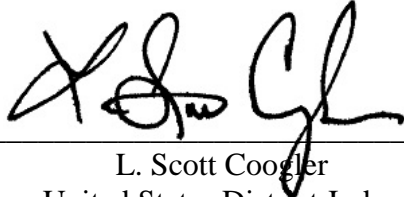
In sum, while several damages claimed by Standifer are not legally cognizable, she has presented sufficient evidence that other categories of damages

are not the result of fear of future harm. Therefore, Standifer's remaining claims are not due to be dismissed for lack of damages.

IV. CONCLUSION

For the reasons stated above, Standifer's motion for partial summary judgment (doc. 37) is due to be GRANTED in PART and DENIED in PART and Best Buy's motion for summary judgment (doc. 39) is also due to be GRANTED in PART and DENIED in PART. An order consistent with this opinion will be entered contemporaneously herewith.

DONE and **ORDERED** on January 30, 2019.



L. Scott Coogler
United States District Judge

194800